Unconditionally Secure Quantum Bit Commitment*

Horace P. Yuen†
*Department of Electrical and Computer Engineering, Department of Physics and Astronomy,
Northwestern University, Evanston, IL 60208-3118, USA*

The "impossibility proof" on unconditionally secure quantum bit commitment is examined. It is shown that the possibility of juxtaposing quantum and classical randomness has not been properly taken into account. A specific protocol that beats entanglement cheating with entanglement is proved to be unconditionally secure.

Bit commitment is a kind of a cryptographic protocol that can serve as a building block to achieve various cryptographic objectives, such as user authentication. There is a nearly universal acceptance of the general impossibility of secure quantum bit commitment (QBC), taken to be a consequence of the Einstein-Podolsky-Rosen (EPR) type entanglement cheating which supposedly rules out QBC and other quantum protocols that have been proposed for various cryptographic objectives. In a *bit commitment* scheme, one party, Adam, provides another party, Babe, with a piece of evidence that he has chosen a bit b (0 or 1) which is committed to her. Later, Adam would *open* the commitment by revealing the bit b to Babe and convincing her that it is indeed the committed bit with the evidence in her possession and whatever further evidence Adam then provides, which she can *verify.* The usual concrete example is for Adam to write down the bit on a piece of paper, which is then locked in a safe to be given to Babe, while keeping for himself the safe key that can be presented later to open the commitment. The scheme should be *binding*, i.e., after Babe receives her evidence corresponding to a given bit value, Adam should not be able to open a different one and convince Babe to accept it. It should also be *concealing*, i.e., Babe should not be able to tell from her evidence what the bit b is. Otherwise, either Adam or Babe would be able to cheat successfully.

In standard cryptography, secure bit commitment is to be achieved either through a trusted third party, or by invoking an unproved assumption concerning the complexity of certain computational problems. By utilizing quantum effects, specifically the intrinsic uncertainty of a quantum state, various QBC schemes not involving a third party have been proposed to be unconditionally secure (US), in the sense that neither Adam nor Babe could cheat with any significant probability of success as a matter of physical laws. In 1995-1996, a supposedly general proof of the impossibility of unconditionally secure QBC, and the insecurity of previously proposed protocols, were presented [1]-[5]. Henceforth it has been generally accepted that secure QBC and related objectives are impossible as a matter of principle [6]-[11].

There is basically just one impossibility proof (IP), which gives the EPR attacks for the cases of equal and unequal density operators that Babe has for the two different bit values. The proof purports to show that if Babe's successful cheating probability P_c^B is close to the value 1/2, which is obtainable from pure guessing of the bit value, then Adam's successful cheating probability P_c^A is close to the perfect value 1. The impossibility proof describes the EPR attack on a specific type of protocols, and then argues that all possible QBC protocols are of this type. Since there is no mathematical characterization of all possible QBC protocols - no mathematical definition of a QBC protocol exists with the justification that it includes all protocols that would achieve bit commitment - a priori there can be no general impossibility proof. A general analysis of the situation is provided in [12]. In this paper, we pinpoint the gaps in the IP involving quantum versus classical randomness that make possible a relatively simple QBC protocol that utilizes classical random numbers generated in any usual way. This particular protocol depends critically on verifying split entangled pairs used as *anonymous states* [13, 14] which Babe first transmitted to Adam in a two-stage protocol, thus beating entanglement with entanglement [16].

The impossibility proof, in its claimed generality, has never been systematically spelled out in one place, but the essential ideas that constitute this proof are generally agreed upon [2]-[11]. The formulation and the proof can be cast as follows. Adam and Babe have available to them two-way quantum communications that terminate in a finite number of exchanges, during which either party can perform any operation allowed by the laws of quantum physics, all processes ideally accomplished with no imperfection of any kind. During these exchanges, Adam would have committed a bit with associated evidence to Babe. It is argued that, at the end of the commitment phase, there is an entangled pure state $|\Phi_{\mathsf{b}}\rangle$, $\mathsf{b} \in \{0,1\}$, shared between Adam who possesses state space $\mathcal{H}^A$, and Babe who possesses $\mathcal{H}^B$. For example, if Adam sends Babe one of M possible states $\{|\phi_{\mathsf{b}i}\rangle\}$ for bit b with probability $p_{\mathsf{b}i}$, then

$$|\Phi_{\mathsf{b}}\rangle = \sum_i \sqrt{p_{\mathsf{b}i}}|e_i\rangle|\phi_{\mathsf{b}i}\rangle \tag{1}$$

with orthonormal $|e_i\rangle \in \mathcal{H}^A$ and known $|\phi_{\mathsf{b}i}\rangle \in \mathcal{H}^B$.

*NOTE: This paper is an expanded, self-contained version of QBC4 presented in quant-ph 0305143. It is the basis of talks to be presented at the University of Pavia, Italy on May 23, 2005 and Nottingham University, England on May 25, 2005.

†Electronic address: yuen@ece.northwestern.edu

Adam would open by making a measurement on $\mathcal{H}^A$, say $\{|e_i\rangle\}$, communicating to Babe his result i_0 and b; then Babe would verify by measuring the corresponding projector $|\phi_{\mathsf{b}i_0}\rangle\langle\phi_{\mathsf{b}i_0}|$ on $\mathcal{H}^B$, accepting as correct only the result 1. More generally, one may consider the whole $|\Phi_{\mathsf{b}}\rangle$ of (1) as the state corresponding to the bit b, with Adam sending $\mathcal{H}^A$ to Babe upon opening, so she can verify by projection measurement on $|\Phi_{\mathsf{b}}\rangle\langle\Phi_{\mathsf{b}}|$.

Classical random numbers are routinely used in classical cryptographic protocols, and so must be allowed in a quantum protocol. In the IP, they are handled as follows. When classical random numbers known only to one party are used in the commitment, they are to be replaced by corresponding quantum state purification. The commitment of $|\phi_{\mathsf{b}i}\rangle$ with probability $p_{\mathsf{b}i}$ in (1) is, in fact, an example of such purification. Generally, for any random k used by Babe, it is argued that from the doctrine of the "Church of the Larger Hilbert Space" [9], it is to be replaced by the purification $|\Psi\rangle$ in $\mathcal{H}^B \otimes \mathcal{H}^B$,

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}|\psi_k\rangle|f_k\rangle, \qquad (2)$$

where $|\psi_k\rangle \in \mathcal{H}^B$ and the $|f_k\rangle's$ are complete orthonormal in $\mathcal{H}^B$ kept by Babe while $\mathcal{H}^C$ would be sent to Adam. With such purification, it is claimed that any protocol involving classical secret parameters would become quantum-mechanically determinate, i.e., the shared state $|\Phi_{\mathsf{b}}\rangle$ at the end of commitment is completely known to both parties. This means that both $\{\lambda_k\}$ and $\{|f_k\rangle\}$ are taken to be known exactly to both Babe *and Adam*. The IP assumes that Babe is honest (and Adam is also honest in a multi-stage protocol [11, 17],[3]) in using the agreed upon $\{\lambda_k\}$ and $\{|f_k\rangle\}$, and then claims that unconditional security is impossible. We will retain this assumption in this paper to show that the IP reasoning is incorrect. However, US QBC is possible even when this assumption is dropped by using a cheat-testing procedure [14, 16].

In the purification (2), exactly which orthonormal $\{|f_k\rangle\}$ is used does not affect the anonymous nature of $\{|\psi_k\rangle\}$. Why then does $\{|f_k\rangle\}$ have to be agreed upon and known to Adam? This issue is *not* addressed in the IP. Clearly, a choice from a set of possible $\{|f^l_k\rangle\}, l \in \{1, \cdots, L\}$ with a priori probabilities $\{p^l\}$, both openly known, can be picked secretly by Babe using a classical random number generator for each transmission of $|\Psi\rangle$. If the protcol is concealing for every l, Adam has no right to demand the knowledge of l. On the other hand, the IP may *not* go through as $\{|f_k\rangle\}$ or the total

$$|\Phi_{\mathsf{b}}\rangle = \sum_{ik} \sqrt{p_{\mathsf{b}i}\lambda_k}|e_i\rangle|f_k\rangle|\phi_{\mathsf{b}ik}\rangle \qquad (3)$$

is *not* known to Adam. This is the anonymous state idea [13, 14] for building US QBC protocols. It should be noted that if Babe, e.g., picks $\{|\psi_k\rangle\}$ by throwing a die with probabilities $\{\lambda_k\}$, she herself would not be able to tell what the $\{|f_k\rangle\}$ is. Thus, physically, it is totally unreasonable to assume that Adam knows the $\{|f_k\rangle\}$ in an anonymous state protocol. Similarly, as just noted, Babe may just send a classically randomly chosen $\{|\psi_k\rangle\}$ so long as the protocol is concealing for every k. As it turns out [14], if the protocol is perfectly concealing ($P^B_c = 1/2$), Adam's cheating transformation U^A on $\mathcal{H}^A$ that brings $|\Phi_0\rangle$ to $|\Phi_1\rangle = U^A \otimes I^B|\Phi_0\rangle$ is independent of $\{|f_k\rangle\}$ or the specific $|\psi_k\rangle$, under either of the following conditions: (a) Babe verifies by first measuring $\{|f_k\rangle\}$ and then checking $|\psi_k\rangle$, or (b) Adam's b-dependent commitment action does not change the composite index k to get one unknown state to another unknown state for him. One way, among others, to show this is to use the result in [14] that explicitly determines U^A in terms of $|\Phi_{\mathsf{b}}\rangle$ of (1) or (3), which can be achieved by a simple matrix transformation argument [15]. Let $U_{ij} \equiv \langle e_i|U^A|e_j\rangle, \Lambda_{ji} \equiv \sqrt{p_ip_j}\langle\phi_{1i}|\phi_{0j}\rangle, |\Lambda| = (\Lambda\Lambda^\dagger)^{1/2}$. Then [14, 15]

$$\Lambda U = |\Lambda|. \qquad (4)$$

Generalization to ϵ-concealing ($P^B_c = 1/2 + \epsilon$) protocols of this behavior can be expected.

However, a perfectly concealing US protocol may be obtained from the use of (2) with $|\psi_k\rangle$ being an entangled state split between Adam and Babe during commitment with Adam's b-dependent commitment action changing the composite index k, while verification is carried out on the total entangled $|\psi_k\rangle$. Such a split entangled state by itself does not lead to a binding protocol for known$\{|f_k\rangle\}$, but together with the use of a secretly chosen $|f^l_k\rangle$ as described above, Adam would not be able to cheat perfectly ($P^A_c = 1$). Thus, an ϵ-binding protocol for any $\epsilon > 0$ is obtained in a sufficiently long n-sequence in the standard fashion [3]. In the following, we describe the specific protocol (which we call QBC4) that achieves unconditional security in the above fashion.

Let $|m_j\rangle_j$, $j \in \{\mu, \nu\}$, $m_j \in \{1, 2\}$, be two openly known orthonormal qubit states, $\langle 1|2\rangle = 0$, for each of the two possible j. When there is no ambiguity, we would write $|m_j\rangle_j$ simply as $|m\rangle_j$ to simplify notation. Let Babe prepare two states

$$|\Psi_j\rangle = \frac{1}{\sqrt{2}} \sum_m |m\rangle_j|g_m\rangle_j, \qquad (5)$$

where $|m\rangle_j \in \mathcal{H}^B_{j\alpha}$, $m \in \{1, 2\}$, and $\{|g_m\rangle_j|m = 1, 2\}$ form an orthonormal basis in $\mathcal{H}^B_{j\beta}$ for each $j \in \{\mu, \nu\}$, with $|\Psi_j\rangle \in \mathcal{H}^B_{j\alpha} \otimes \mathcal{H}^B_{j\beta}$ on two qubits for each j. We have skipped one subscript j in $|g_{m_j}\rangle_j$ as in $|m\rangle_j$ to simplify notation. Let $\mathcal{H}^B_\alpha \equiv \mathcal{H}^B_{\mu\alpha} \otimes \mathcal{H}^B_{\nu\alpha}$, $\mathcal{H}^B_\beta \equiv \mathcal{H}^B_{\mu\beta} \otimes \mathcal{H}^B_{\nu\beta}$, $\mathcal{H}^B \equiv \mathcal{H}^B_\alpha \otimes \mathcal{H}^B_\beta$.

Babe keeps $\mathcal{H}^B_\beta$ and sends the ordered pair of qubits $\mathcal{H}^B_\alpha$ to Adam. Adam applies the following transformation on $\mathcal{H}^B_{j\alpha}$ separately for each j: $|\Psi_j\rangle$ becomes $|\Phi_j\rangle \in \mathcal{H}^A_j \otimes \mathcal{H}^B_{j\alpha} \otimes \mathcal{H}^B_{j\beta}$:

$$|\Phi_j\rangle = \frac{1}{\sqrt{8}} \sum_{m,i} |e_i\rangle_j V_i|m\rangle_j|g_m\rangle_j, \qquad (6)$$

where $i \in \{1,2,3,4\}$, $\{|e_i\rangle_j\}$ complete orthonormal in $\mathcal{H}^A_j$, and V_i are four unitary qubit operators given by I, σ_x, $-i\sigma_y$, σ_z in terms of the Pauli spin operators when $|1\rangle$ and $|2\rangle$ lie on the qubit z-axis. Eq. (6) can be obtained by the unitary transformation $\sum_i |e_i\rangle_{jj}\langle e_i| \otimes V_i$ on $\mathcal{H}^A \otimes \mathcal{H}^B_{j\alpha}$ with initial state $|\psi_A\rangle \in \mathcal{H}^A$ that has $\langle e_i|\psi_A\rangle_j = \frac{1}{2}$. To commit $\mathsf{b}=0$, Adam sends back $\mathcal{H}^B_{\mu\alpha} \otimes \mathcal{H}^B_{\nu\alpha}$ in the original order, and he switches them to $\mathcal{H}^B_{\nu\alpha} \otimes \mathcal{H}^B_{\mu\alpha}$ to commit $\mathsf{b}=1$. He opens by announcing b, the order of the two $\mathcal{H}^B_{j\alpha}$ he committed, and submitting the ordered qubit pair $\mathcal{H}^A \equiv \mathcal{H}^A_\mu \otimes \mathcal{H}^A_\nu$. Babe verifies by measuring the corresponding projections to $|\Phi_\mu\rangle|\Phi_\nu\rangle$ of (6). The general situation is depicted in Fig. 1.

It is easy to verify by tracing over $\mathcal{H}^A$ that for either b, $\rho^B_0 = \rho^B_1 = I^B/16$ on $\mathcal{H}^B$, for any orthonormal $\{|g_m\rangle_j\}$. If Babe entangles over the possible choices of such $\{|g_m\rangle_j\}$ via $\{|f_k\rangle\}$, a simple calculation shows that perfect concealing $\rho^{BC}_0 = \rho^{BC}_1$ on $\mathcal{H}^B \otimes \mathcal{H}^C$ is maintained, where $\mathcal{H}^C$ is the space Babe used to carry out such entanglement. Similarly, pefect concealing is maintained with further entanglement of $\{|f^l_k\rangle\}$ with $\{p^l\}$. This happens because the V_i operations by Adam totally disentangle the state on $\mathcal{H}^B_\alpha \otimes \mathcal{H}^B_\beta \otimes \mathcal{H}^C$ into a product state $I^B_\alpha/4 \otimes \rho^{BC}_\beta$ for either b, and there is no identity that individuates a qubit by itself, that is not entangled or correlated to another.

Intuitively, we intend to guarantee binding by the fact that $\mathcal{H}^B_{j\beta} = \mathcal{H}^B_{\mu\beta} \otimes \mathcal{H}^B_{\nu\beta}$ in Babe's possession cannot be switched to $\mathcal{H}^B_{\nu\beta} \otimes \mathcal{H}^B_{\mu\beta}$ by operating on $\mathcal{H}^A \otimes \mathcal{H}^B_\alpha$ alone. However, this is possible if the two orthonormal sets $\{|g_m\rangle_j\}$ are known. Indeed, this is the content of the impossibility proof [18]. Thus, to guarantee security, Babe needs to employ different choices of $\{|g^{k'}_m\rangle_j\}$ with different bases indexed by k'. She may employ a fixed probability distribution $\{p_{k'j}\}$ for each j, and entangle these via orthonormal $\{|g^{k'}\rangle_j\}$, ad infinitum. This possible chain of purifications has to stop somewhere, and we simply stop it at $\mathcal{H}^B$ without $\mathcal{H}^C$. As we have seen, this does not affect perfect concealing so that Babe is free to choose any orthonormal $\{|g_m\rangle_j\}$. In the notation of (2), the effective $\{|\psi_k\rangle\}$ in this case is $|\Psi^{k'}_\mu\rangle|\Psi^{k'}_\nu\rangle$ determined by $\{|g^{k'}_m\rangle\}$, with further entanglement to $|f_k\rangle$ of (2) described by $\mathcal{H}^C$ above. In the notation of (2), k is the ordered triple (μ,ν,k') for fixed $\{|g^{k'}_m\rangle\}$. It is clearly unreasonable for Adam to demand such knowledge, as discussed above and codified in the Secrecy Principle of Ref. [18]. This possibility is neglected in the impossibility proof.

To see exactly how binding is obtained in the present situation, note that the perfect cheating transformation U^A is determined by Eq. (4), which is unique up to a phase factor in this nondegenerate situation. It depends on $\{|g_m\rangle_j\}$ in the present case with state-space switching, i.e. μ,ν-switching where $\{\mu,\nu\}$ is part of the composite index k, in contrast to merely $\langle g_m|g_{m'}\rangle = \delta_{mm'}$, i.e., no dependence on the actual $\{|g_m\rangle\}$ in the case without switching in the absence of j. Thus, Adam cannot cheat perfectly. Note that the generalized IP result from [14] does not apply here because Adam's b-dependent commitment action re-arranges the μ,ν part of the composite index k of (2), which in turn demands entanglement or correlation from Babe in order that she can verify such re-arrangement. On the other hand, quantum entanglement instead of classical correlation is also needed here – Babe cannot verify by first measuring $\{|m\rangle_j\}$ because Adam would be able to determine the $|m\rangle_j$ with a measurement if he knows that is the way Babe would verify. Thus, we are indeed beating entanglement with entanglement. On the other hand, Adam's entanglement is not essential. As usual in QBC protocols, the whole procedure works the same if Adam chooses the V_i on $\mathcal{H}^B_{\mu\alpha}$ and $\mathcal{H}^B_{\nu\alpha}$ classically and opens by telling Babe his choice.

We have assumed as usual that Adam opens $\mathsf{b}=0$ perfectly. Let $p_A < 1$ be Adam's optimum probability of cheating for a given choice of $\{|g^{k'}_m\rangle_j\}$ and $\{p_{k'j}\}$, taking into account also all his other obvious imperfect cheating possibilities, such as simply announcing a different b. We have thus shown that the formulation and the reasoning of the impossibility proof break down already in this simple pair $|\Phi_\mu\rangle|\Phi_\nu\rangle$ situation.

When $\mathsf{b}=0$ pefect opening condition is relaxed, it is clear that Adam still cannot cheat perfectly, but it is possible that the overall successful opening probability (honest plus cheating) may be improved. By continuity it can be seen that Adam's optimum cheating probability $\bar{P}^A_c$ is arbitrarily close to $p_A = \frac{1}{2}$ if the $\mathsf{b}=0$ opening probability is arbitrarily close to 1, the case of interest.

Protocol QBC4 is obtained when the above protocol, to be called QBC4p, is extended to a sequence of $\{|\Psi_{n\mu}\rangle|\Psi_{n\nu}\rangle\}$, $n \in \{1,\ldots,N\}$, each of the form (5), with $|g_{nm}\rangle_j \in \mathcal{H}^B_{nj\beta}$, $|m_n\rangle_j \in \mathcal{H}^B_{nj\beta}$, etc. Babe should send Adam $\{\mathcal{H}^B_{n\mu\alpha} \otimes \mathcal{H}^B_{n\nu\alpha}\}$ and Adam should commit to Babe these spaces for all μ after he entangles them with $\mathcal{H}^A_{n\mu} \otimes \mathcal{H}^A_{n\nu}$ using the V_i operations, permuting each pair for $\mathsf{b}=1$. He opens by announcing b and the state of the qubits in each $\mathcal{H}^B_{n\alpha}$ and submitting $\{\mathcal{H}^A_n\}$, with Babe verifyng $|\Phi_{n\mu}\rangle|\Phi_{n\nu}\rangle \in \mathcal{H}^A_n \otimes \mathcal{H}^B_n$ after possible rearrangement for each n. Since there is no new entanglement possibility for Adam, the protocol is perfectly concealing with $\bar{P}^A_c = p^n_A$ going to zero exponentially in N. Thus, QBC4 is perfectly concealing and ϵ-binding for any $\epsilon > 0$ by letting N be large. We summarize our perfectly concealing and ϵ-binding protocol:

PROTOCOL **QBC4**

(i) Babe sends Adam N ordered pairs $\{\mathcal{H}^B_{n\mu\alpha} \otimes \mathcal{H}^B_{n\nu\alpha}\}$ of qubit pairs, $n \in \{1,\ldots,N\}$, which are entangled to $\{\mathcal{H}^B_{n\mu\beta} \otimes \mathcal{H}^B_{n\nu\beta}\}$ in her possession in states $|\Psi_{n\mu}\rangle|\Psi_{n\nu}\rangle$ of the form (5), with independent random choices of $\{|g^{k'}_m\rangle_j\}$ with probability $\{p_{k'j}\}$.

(ii) To commit b, Adam applies, for each n, $\sum_i |e_i\rangle\langle e_i| \otimes V_i$ on $\mathcal{H}^A_n \otimes \mathcal{H}^B_{n\alpha}$, resulting in a state $|\Phi_{n\mu}\rangle|\Phi_{n\nu}\rangle$ given via the form (6), and sends $\{\mathcal{H}^B_{n\alpha}\}$ to Babe as evidence for $\mathsf{b} = 0$, while switching the order ot each $\mathcal{H}^B_{n\mu\alpha} \otimes \mathcal{H}^B_{n\nu\alpha}$ for $\mathsf{b} = 1$.

(iii) Adam opens by announcing b, the order of the qubits in each $\mathcal{H}^B_{n\alpha}$, and submitting $\{\mathcal{H}^A_n\}$. Babe verifies by projective measurements of $\{|\Phi_{n\mu}\rangle\}$, $\{|\Phi_{n\nu}\rangle\}$, for all n.

In conclusion, the possibility of unconditionally secure quantum bit commitment opens up the possibility of many cryptographic functions, including secure multi-party computation. It would be of interest to develop practically feasible secure QBC protocols [12] for such applications.

Acknowledgments

I would like to thank G.M. D'Ariano, W.Y. Hwang, and R. Nair for useful discussions. This work was supported by the Defense Advanced Research Projects Agency and by the U.S. Army Research Office.

[1] D. Mayers, preprint quant-ph/9603015.

[2] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[3] H.K. Lo and H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[4] H.K. Lo and H.F. Chau, Fortschr. Phys. **46**, 907 (1998).

[5] H.K. Lo and H.F. Chau, Physica D **120**, 177 (1998).

[6] H.K. Lo, Phys. Rev. A **56**, 1154 (1997).

[7] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, preprint quant-ph/9712023.

[8] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, preprint quant-ph/9806031.

[9] D. Gottesman and H.K. Lo, Physics Today, Nov. 2000, p. 22.

[10] J. Mueller-Quade and H. Imai, preprint quant-ph/0010112.

[11] R.W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).

[12] H.P. Yuen, preprint quant-ph/0305144

[13] H.P. Yuen, in *Quantum Communication, Computation and Measurement* 3, ed by P. Tombesi and O. Hirota, Plenum, New York, 2001, p. 285

[14] H.P. Yuen, preprint quant-ph/0109055

[15] The maximum of $|\langle\Phi_1|U^A|\Phi_0\rangle| = |trU\Lambda|$ over all unitary U is obtained when $U\Lambda$ is nonnegative definite with maximum value given by $tr|\Lambda| = \bar{P}^A_c$. Thus U is determined by the polar decomposition of $\Lambda = |\Lambda|U^\dagger$.

[16] H.P. Yuen, preprint quant-ph/0305143.

[17] I would like to thank G.M. D'Ariano for bringing this to my attention.

[18] H.P. Yuen, quant-ph/0210206. Also in Proceedings of the Sixth International Conference on *Quantum Communication, Measurement, and Computing*, ed. by J.H. Shapiro and O. Hirota, Rinton, pp.371-376 (2003).